OFFICE OF THE LIEUTENANT GOVERNOR
State Capitol, Fifth Floor
Honolulu, Hawaii 96813
Phone: (808)586-0255
Fax: (808)586-0231
email: ltgov@hawaii.gov
www.hawaii.gov/ltgov

JAMES R. AIONA, JR.
LIEUTENANT GOVERNOR

May 20, 2009

MEMORANDUM

TO: Russ K. Saito, State Comptroller
Department of Accounting and General Services

FROM: Kevin A. Souza KS
Chief of Staff

RE: Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers

Attached is the Office of the Lieutenant Governor's response to your Memorandum dated April 23, 2009, wherein you requested that our office provide a plan to eliminate the unnecessary collection and use of social security numbers.

If you should have any further questions, you may contact Ms. Dawn Matsumura, our Administrative Services Specialist or myself at (808) 586-0255.

Office of the Lieutenant Governor

Personal Information Procedure Plan

In accordance with Act 135 Notification of Security Breaches, Act 136 Destruction of Personal Information Records, Act 137 Social Security Number Protection, Session Laws of Hawaii 2006, and Act 10 Part VII Section 11, Session Laws of Hawaii 2008, requires all government agencies to develop a written plan to eliminate the unnecessary collection and use of social security numbers. This plan shall include, but are not limited to:

Department Policy:

1. All records containing "personal information" as defined in Acts 135 and 136 are to be shredded, erased, or otherwise destroyed before they are discarded;

2. The use of social security numbers on forms and in computer applications including the internet, will be limited to the uses allowed by Act 137; and

3. Any instance of possible unauthorized access to records containing such personal information must be immediately reported to the Chief of Staff, division administrator, staff officer or attached agency director. The Chief of Staff or appropriate administrator will evaluate the incident and determine the appropriate response.

For the specific purposes of the Department's Policy, "personal information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following, when either the name or data elements are not encrypted:

1. Social Security number;

2. Driver's license number or Hawaii identification number; or

3. Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Office Procedures:

1. Conduct a review of the collection and use of social security numbers in order to determine the circumstances under which their use as a primary identifier may be eliminated, restricted, or concealed in the agencies system and forms (paper or electronic).

2. Remove or suppress social security numbers in databases that are shared unless required by law, or deemed necessary.

3. Remove social security numbers from all physical verification materials unless required by law, or deemed necessary.

4. Ensure that paper documents displaying social security numbers are maintained and disposed of, in accordance with agency policy; and maintained in a manner that limits access only to authorized persons throughout the documents lifecycle.

5. Develop a process to ensure that social security numbers are not collected, used or disseminated unless authorized by law, deemed necessary or a compelling need is shown.

6. Inventory all forms that require social security numbers, and evaluate use of social security numbers on these forms to ensure use is essential to their business purpose, and collaborate with internal and external agencies as necessary to ensure changes are evaluated and issues resolved to ensure continuity.

7. Conduct periodic audits of contracts dealing with the collection and use of social security numbers for compliance with this Act.

8. Employees must notify the appropriate administrator immediately after they become aware that personal information has not been destroyed and/or unauthorized use or access has occurred in accordance with the department's policy.

Updates to this plan will be submitted as it becomes necessary.